What is claimed is:

1. An automated encryption system for encrypting an electronic message from a sender to a recipient comprising:

a computer readable medium;

a network port in communication with said computer readable medium for accessing a set of public key data having a public key associated with the recipient,

a set of computer readable encryption instructions embodied in said computer readable medium for:

receiving said electronic message from the sender addressed to the recipient,

retrieving said public key associated with the recipient from said public key data via said network connection,

encrypting said electronic message according to said public key associated with the recipient, and,

forwarding said encrypted message to the recipient for subsequent retrieval so that the electronic message is automatically encrypted and delivered to the recipient.

2. The system of claim 1 including:

a set of private key data embodied in said computer readable medium having a private key associated with the sender; and,

said set of computer readable encryption instructions include instructions for:

retrieving said private key associated with the sender from said set of

private key data, and,

signing said electronic message from the sender according to said private key associated with the sender so that the recipient can verify the authenticity of said electronic message.

3. The system of claim 1 including:

a set of private key data contained within said computer readable medium having a private key associated with the sender; and,

a set of computer readable access instructions embodied in said computer readable medium for:

receiving an access attempt input from the sender,

retrieving said private key associated with the sender from said set of private data,

validating said access attempt input according to said private key to determine whether a valid access attempt input has been provided, and,

encrypting said electronic message according to said public key if said access attempt input is valid so that only senders with valid access attempt inputs may send encrypted messages.

4. The system of claim 3 wherein said set of computer readable access instructions include instructions for signing said electronic message using said private key associated with the sender so that said electronic message can be authenticated.

5. The system of claim 1 including:

a set of private key data contained within said computer readable medium,

a set of computer readable key maintenance instruction embodied within said computer readable medium for:

creating a key pair having said at least one public key associated with the senders, and,

a private key associated with said public key and the sender,

storing said public key within said set of public key data so that said public key associated with the sender is available for retrieval,

storing said private key within said private key data so that the sender can retrieve said private key for decrypting message sent to the sender, and,

deleting said key pair to prevent the sender from decrypting encrypted messages so that an automated key management system is provided for automatically managing key pairs for senders.

6. The system of claim 5 including a set of public key data embodied within said computer readable medium.

7. The system of claim 1 including:

a set of encrypted private key data contained within said computer readable medium;

a set of computer readable key maintenance instruction embodied within said computer readable medium for:

creating a key pair having said at least one public key associated with the sender and a private key associated with said public key and the sender,

storing said public key within said set of public key data so that said

public key associated with the sender is available for retrieval,

receiving a password from the sender,

encrypting said private key according to said password,

storing said encrypted private key within said private key data so that the sender can retrieve said private key for decrypting message sent to the sender, and,

deleting said key pair to prevent the sender from decrypting encrypted messages so that an automated key management system is provided for automatically managing key pairs for senders.

8. An automated encryption system for decrypting an electronic message from a sender to a recipient comprising:

a computer readable medium;

a set of private key data embodied within said computer readable medium having a private key associated with the recipient;

a set of computer readable decryption instructions embodied within said computer readable medium for:

receiving said electronic message from the sender to the recipient,

retrieving said private key associated with the recipient from said set of private key data,

decrypting said electronic message according to said private key, and,

providing said decrypted message to the recipient so that the recipient automatically retrieves and decrypts an electronic encrypted message without

manually managing private keys.

9. The system of claim 8 including:

a network port in communication with said computer readable medium for accessing a set of public key data having a public key associated with the sender;

a set of computer readable message verification instructions embodied within said computer readable medium for:

receiving said encrypted message having a digital signature associated with the sender,

retrieving said public key associated from the sender from said digital signature,

validating said electronic message according to said digital signature to provide validation information, and,

providing the resulting validation information to the recipient so that the recipient can be notified as to the authenticity of the received encrypted message.

10. The system of claim 8 including:

a network port in communication with said computer readable medium for accessing a set of public key data; and,

a set of computer readable key maintenance instructions embodied within said computer readable medium for:

creating a key pair having a public key and a private key associated with the recipient,

storing said public key within the set of public key data via said network port,

storing said private key within said set of private key data, and,

deleting said key pair to prevent the recipient from decrypting messages so than an automated key management system is provided for automatically managing key pairs of recipients.

11. The system of claim 10 including a set of public key data embodied within said computer readable medium.

12. The system of claim 10 wherein said set of computer readable maintenance instructions include instruction for:

receiving a password from the sender, and,

encrypting said private key associated with the sender so that said private key can not be used to decrypt messages without supplying an access attempt matching said password.

13. A computerized system for encrypting an electronic message from a sender to a recipient comprising:

a computer readable medium;

a means for receiving an electronic message from a sender to a recipient embodied in said computer readable medium;

a means for obtaining a public key associated with the recipient;

a means for encrypting said electronic message according to said public key; and,

a means for forwarding said encrypted electronic message to the recipient for subsequent decryption and retrieval.

14. The system of claim 13 including:

an encrypted private key associated with the sender encrypted according to a password supplied to the sender and contained within said computer readable medium;

a means for receiving an access attempt from the sender; and,

a means for validating said access attempt according to said encrypted private key so that said electronic message is not encrypted unless said access attempt is valid.

15. The system of claim 13 including:

a means for informing the sender that said public key associated with the recipient cannot be found so that electronic message cannot be encrypted; and,

a means for sending said electronic message to the recipient.

16. The system of claim 13 including:

a computer readable medium;

a means for receiving an encrypted electronic message from the sender to the recipient;

a means for obtaining a private key associated with the recipient;

a means for decrypting said encrypted electronic message from the sender to the recipient so that the recipient can receive and decrypt an encrypted message.

17. The system of claim 13 including:

a digital signature associated with the sender contained within said computer readable medium; and,

a means for signing said electronic message with said digital signature.

18. The system of claim 13 including:

a means for receiving an electronic message having a digital signature associated with the sender; and,

a means for verifying the authenticity of said electronic message according to said digital signature so that the recipient is ensured that said electronic message truly originates from the sender.

19. An automated encryption system for decrypting an electronic message from a sender to a recipient comprising:

a computer readable medium;

a set of encrypted private key data embodied within said computer readable medium having an encrypted private key associated with the recipient encrypted according to a password supplied by the sender;

a set of computer readable decryption instructions embodied within said computer readable medium for:

receiving said electronic message from the sender to the recipient,

retrieving said encrypted private key associated wit the recipient from said set of private key data,

attempting to decrypt said private key according to said access attempt input so that said access attempt input can be validated,

decrypting said electronic message according to said private key if said access attempt input is valid, and,

providing said decrypted message to the recipient so that the recipient automatically retrieves and decrypts an electronic encrypted message without manually managing private keys.